(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－500923
（P2003－500923A）
(43)公表日　平成15年１月７日(2003.1.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６７５Ｂ	５Ｊ１０４
Ｈ０４Ｌ　9/08			６０１Ｆ	

審査請求　有　　予備審査請求　有　（全 53 頁）

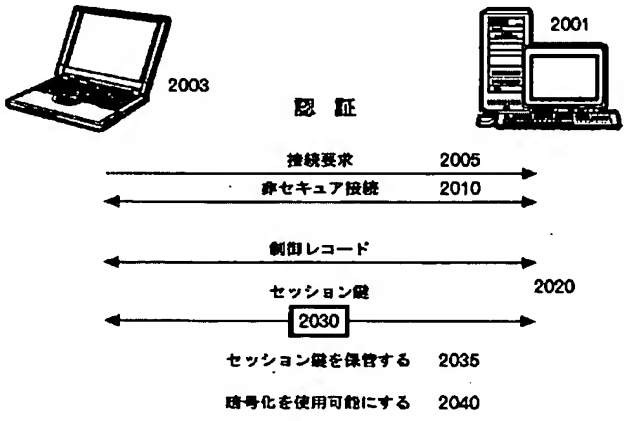
(21)出願番号　特願2000－619855(P2000－619855)
(86)（22)出願日　平成12年５月22日(2000.5.22)
(85)翻訳文提出日　平成13年11月20日(2001.11.20)
(86)国際出願番号　ＰＣＴ／ＧＢ００／０１９４０
(87)国際公開番号　ＷＯ００／０７２５０６
(87)国際公開日　平成12年11月30日(2000.11.30)
(31)優先権主張番号　０９／３１６，８０５
(32)優先日　平成11年５月21日(1999.5.21)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／３１６，８０４
(32)優先日　平成11年５月21日(1999.5.21)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(72)発明者　ヒンド、ジョン、ライテル
アメリカ合衆国27613　ノースカロライナ州ローリー　ハリントン・グローブ・ドライブ　5408
(74)代理人　弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　セキュア通信をイニシャライズし、装置を排他的にペアリングする方法、コンピュータ・プログラムおよび装置

(57)【要約】
【課題】　無線ネットワーク内でモバイル装置の間のセキュア通信を効率的に確立する方法およびシステム。
【解決手段】　本発明は、公開鍵暗号および固有のハードウェア識別子を使用して、ピコセルなどの無線ネットワークへのアクセスの許可を可能にする。本発明は、モバイル・ユーザが、ユーザ識別子／パスワード対、ＰＩＮ、または暗号化鍵などの複数の秘密を、アクセスを必要とする可能性がある装置のそれぞれへのアクセスのために維持する必要をなくす。企業全体に配布された無線装置を、セキュア通信のために効率的にイニシャライズできるようになる。周知の公開鍵暗号および機械固有識別子を使用して、セキュア・チャネルを確立し、無線装置をイニシャライズする。無線装置を、ユーザまたはネットワーク管理者がペアリングするか永久的に関連付けることができる。周知の公開鍵暗号および機械固有識別子を使用して、セキュア・チャネルを確立し、装置を互いに関連付ける。これは、無線ヘッドセットと電話機の関連付けまたは無線マウスとコンピュータの関連付けに非常に有用である。



【特許請求の範囲】

【請求項１】

第１装置と第２装置との間でセキュア通信をイニシャライズする方法であって、前記第１装置および前記第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、前記装置証明書がそれぞれの前記装置に関連付けられた固有ハードウェア識別子およびそれぞれの前記装置に関連付けられた公開鍵を有し、

前記第１装置と前記第２装置との間のセッションを確立するステップと、

前記第１装置と前記第２装置との間で両方向セッション暗号化および相互認証要件をネゴシエートするステップと、

前記第１装置および前記第２装置の装置証明書を交換するステップと、

前記認証局の前記公開鍵を使用して受信された前記証明書を暗号的に検証するステップと、

前記第１装置および前記第２装置のそれぞれによって作成されたチャレンジを交換するステップと、

受信側装置の秘密鍵を使用して受信された前記チャレンジに署名することによってそれぞれの前記チャレンジに応答するステップであって、前記秘密鍵が各前記装置の保護された記憶装置それぞれに常駐する、ステップと、

署名された前記チャレンジを返すステップと、

受信された前記チャレンジ署名が前記受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証するステップと、

前記第１装置と前記第２装置との間で鍵合意を確立するステップと、

前記検証するステップのすべてに成功する場合にセキュア通信を確立するステップと

を含む方法。

【請求項２】

前記保護された記憶装置が読取書込記憶装置であり、前記記憶装置の読取が共用される秘密によってのみアクセス可能となっている、請求項１に記載の方法。

【請求項３】

サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシ

ャライズする方法であって、前記サーバが組込み無線機モジュールを有し、

前記組込み無線機モジュールを使用して、前記サーバから前記第１装置に照会を送信するステップと、

前記第１装置から前記サーバに、前記第１装置の固有装置識別子を返すステップと、

前記サーバで、前記第１装置の公開鍵／秘密鍵対を作成するステップと、

前記サーバで、前記第１装置の装置証明書を作成するステップであって、前記装置証明書が前記第１装置に関連付けられた固有ハードウェア識別子および前記第１装置に関連付けられた公開鍵を有する、ステップと、

前記第１装置に、前記秘密鍵、前記装置証明書、および前記装置証明書に署名した認証局の公開鍵を送信するステップと、

前記秘密鍵を前記第１装置の取外し不能な保護された記憶装置に記憶するステップと

を含む方法。

【請求項４】

前記証明書のコピーが企業データベースに記憶される、請求項３に記載の方法。

【請求項５】

前記証明書のコピーがＬＤＡＰディレクトリに記憶される、請求項３に記載の方法。

【請求項６】

サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズする方法であって、前記サーバが組込み無線機モジュールを有し、

前記組込み無線機モジュールを使用して、前記サーバから前記第１装置に照会を送信するステップと、

前記第１装置で、前記第１装置の公開鍵／秘密鍵対を作成するステップと、

前記第１装置で、前記秘密鍵を取外し不能な保護された記憶装置に記憶するステップと、

前記第１装置から前記サーバに、前記第１装置の固有装置識別子および前記公

開鍵を返すステップと、

前記サーバで前記第１装置の装置証明書を作成するステップであって、前記装置証明書が前記装置識別子および前記公開鍵を有する、ステップと

前記装置証明書および前記装置証明書に署名した認証局の公開鍵を前記第１装置に送信するステップと

を含む方法。

【請求項７】

前記保護された記憶装置が前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、請求項１、請求項３、または請求項６に記載の方法。

【請求項８】

第１装置と第２装置との間でセキュリティ関係を確立する方法であって、前記第１装置および前記第２装置がそれぞれ関連付けられた装置証明書を有し、前記装置証明書のそれぞれが前記対応する装置の固有装置識別子を有し、

前記装置の一方の前記装置の他方へのペアリング要求を開始するステップと、

前記第１装置から前記第２装置に、前記第１装置の前記装置証明書を送信するステップと、

前記第２装置によって、前記第１装置の前記受信された装置証明書を暗号的に検証するステップと、

前記第２装置で、前記第１装置証明書に含まれる前記第１装置の前記装置識別子を出力するステップと、

ユーザによって、前記出力された装置識別子が前記第１装置の固有識別子と一致することを検証するステップであって、前記固有識別子が前記ユーザに既知である、ステップと、

前記ユーザによって、前記表示された装置識別子が検証される場合に、前記第１装置と前記第２装置との関連付けを受け入れるステップと

を含む方法。

【請求項９】

前記送信するステップおよび前記検証するステップが、前記第１装置と前記第

２装置との間で認証されたセキュア・セッションを確立することによって実現される、請求項８に記載の方法。

【請求項１０】

前記第１装置および前記第２装置の関連付けのインジケータが長期記憶装置に配置される、請求項８に記載の方法。

【請求項１１】

前記インジケータが前記装置識別子である、請求項１０に記載の方法。

【請求項１２】

前記インジケータが鍵材料である、請求項１０に記載の方法。

【請求項１３】

前記ペアリング要求が前記装置の１つで入力選択を行うことによって開始される、請求項８ないし１２のいずれか一項に記載の方法。

【請求項１４】

前記ペアリング要求が前記装置の一方が前記装置の他方を自動的に検出することによって開始される、請求項８ないし１２のいずれか一項に記載の方法。

【請求項１５】

前記自動検出が前記装置の一方からの電磁信号の送信および前記装置の他方での前記電磁信号の受信によって達成される、請求項１４に記載の方法。

【請求項１６】

前記関連付けの前記受け入れが前記第２装置で入力選択を行うことによって達成される、請求項８に記載の方法。

【請求項１７】

第１装置と第２装置との間でセキュア通信をイニシャライズするコンピュータ・プログラムであって、前記第１装置および前記第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、前記装置証明書がそれぞれの前記装置に関連付けられた固有ハードウェア識別子およびそれぞれの前記装置に関連付けられた公開鍵を有し、前記装置に、

前記第１装置と前記第２装置との間のセッションを確立する手順と、

前記第１装置と前記第２装置との間で両方向セッション暗号化および相互認証

要件をネゴシエートする手順と、

前記第１装置および前記第２装置の装置証明書を交換する手順と、

前記認証局の前記公開鍵を使用して受信された前記証明書を暗号的に検証する手順と、

前記第１装置および前記第２装置のそれぞれによって作成されたチャレンジを交換する手順と、

受信側装置の秘密鍵を使用して受信された前記チャレンジに署名することによってそれぞれの前記チャレンジに応答する手順であって、前記秘密鍵が各前記装置の保護された記憶装置それぞれに常駐する手順と、

署名された前記チャレンジを返す手順と、

受信された前記チャレンジ署名が前記受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証する手順と、

前記第１装置と前記第２装置との間で鍵合意を確立する手順と、

前記検証するステップのすべてに成功する場合にセキュア通信を確立する手順と

を実行させるコンピュータ・プログラム。

【請求項１８】

前記保護された記憶装置が前に書き込まれたデータを用いる計算を実行する能力を有する書込専用記憶装置である、請求項１７に記載のコンピュータ・プログラム。

【請求項１９】

前記保護された記憶装置が読取書込記憶装置であり、前記記憶装置の読取が共用される秘密によってのみアクセス可能となっている、請求項１７に記載のコンピュータ・プログラム。

【請求項２０】

サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするコンピュータ・プログラムであって、前記サーバが組込み無線機モジュールを有し、前記サーバおよび前記第１装置に

前記組込み無線機モジュールを使用して、前記サーバから前記第１装置に照会

を送信する手順と、

前記第１装置から前記サーバに、前記第１装置の固有装置識別子を返す手順と、

前記サーバで、前記第１装置の公開鍵／秘密鍵対を作成する手順と、

前記サーバで、前記第１装置の装置証明書を作成する手順であって、前記装置証明書が、前記第１装置に関連付けられた固有ハードウェア識別子および前記第１装置に関連付けられた公開鍵を有する手順と、

前記第１装置に、前記秘密鍵、前記装置証明書、および前記装置証明書に署名した認証局の公開鍵を送信する手順と、

前記秘密鍵を前記第１装置の取外し不能な保護された記憶装置に記憶する手順と

を実行させるコンピュータ・プログラム。

【請求項２１】

前記証明書のコピーが企業データベースに記憶される、請求項２０に記載のコンピュータ・プログラム。

【請求項２２】

前記証明書のコピーがＬＤＡＰディレクトリに記憶される、請求項２０に記載のコンピュータ・プログラム。

【請求項２３】

サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするコンピュータ・プログラムであって、前記サーバが組込み無線機モジュールを有し、前記サーバおよび前記第１装置に

前記組込み無線機モジュールを使用して、前記サーバから前記第１装置に照会を送信する手順と、

前記第１装置で、前記第１装置の公開鍵／秘密鍵対を作成する手順と、

前記第１装置で、前記秘密鍵を取外し不能な保護された記憶装置に記憶する手順と、

前記第１装置から前記サーバに、前記第１装置の固有装置識別子および前記公開鍵を返す手順と、

前記サーバで前記第１装置の装置証明書を作成する手順であって、前記装置証明書が前記装置識別子および前記公開鍵を有する手順と

前記装置証明書および前記装置証明書に署名した認証局の公開鍵を前記第１装置に送信する手順と

を実行させるコンピュータ・プログラム。

【請求項２４】

前記保護された記憶装置が、前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、請求項１７、請求項２０、または請求項２３に記載のコンピュータ・プログラム。

【請求項２５】

第１装置と第２装置との間でセキュリティ関係を確立するコンピュータ・プログラムであって、前記第１装置および前記第２装置がそれぞれ関連付けられた装置証明書を有し、前記装置証明書のそれぞれが前記対応する装置の固有装置識別子を有し、前記装置に

前記装置の一方の前記装置の他方へのペアリング要求を開始する手順と、

前記第１装置から前記第２装置に、前記第１装置の前記装置証明書を送信する手順と、

前記第２装置によって、前記第１装置の前記受信された装置証明書を暗号的に検証する手順と、

前記第２装置で、前記第１装置証明書に含まれる前記第１装置の前記装置識別子を出力する手順と、

ユーザによって、前記出力された装置識別子が前記第１装置の固有識別子と一致することを検証する手順であって、前記固有識別子が前記ユーザに既知である手順と、

前記ユーザによって、前記表示された装置識別子が検証される場合に、前記第１装置と前記第２装置との関連付けを受け入れる手順と

を実行させるコンピュータ・プログラム。

【請求項２６】

前記送信する手順および前記検証する手順が、前記第１装置と前記第２装置と

の間で認証されたセキュア・セッションを確立することによって実現される、請求項２５に記載のコンピュータ・プログラム。

【請求項２７】

前記第１装置および前記第２装置の関連付けのインジケータが長期記憶装置に配置される、請求項２５に記載のコンピュータ・プログラム。

【請求項２８】

前記インジケータが前記装置識別子である、請求項２７に記載のコンピュータ・プログラム。

【請求項２９】

前記インジケータが鍵材料である、請求項２７に記載のコンピュータ・プログラム。

【請求項３０】

前記ペアリング要求が前記装置の１つで入力選択を行うことによって開始される、請求項２５ないし２９のいずれか一項に記載のコンピュータ・プログラム。

【請求項３１】

前記ペアリング要求が前記装置の一方が前記装置の他方を自動的に検出することによって達成される、請求項２５ないし２９のいずれか一項に記載のコンピュータ・プログラム。

【請求項３２】

前記自動検出が前記装置の一方からの電磁信号の送信および前記装置の他方での前記電磁信号の受信によって達成される、請求項３１に記載のコンピュータ・プログラム。

【請求項３３】

前記関連付けの前記受け入れが前記第２装置で入力選択を行うことによって達成される、請求項２５に記載のコンピュータ・プログラム。

【請求項３４】

第１装置と第２装置との間でセキュア通信をイニシャライズするシステムであって、前記第１装置および前記第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、前記装置証明書がそれぞれの前記装置に関連付けられた固有ハード

ウェア識別子およびそれぞれの前記装置に関連付けられた公開鍵を有し、

前記第１装置と前記第２装置との間のセッションを確立し、前記第１装置と前記第２装置との間で両方向セッション暗号化および相互認証要件をネゴシエートし、前記第１装置および前記第２装置の装置証明書を交換する通信手段と、

前記認証局の前記公開鍵を使用して前記受信された証明書を暗号的に検証する検証手段と、

前記第１装置および前記第２装置のそれぞれによって作成されたチャレンジを交換し、受信側装置の秘密鍵であって、各前記装置の保護された記憶装置それぞれに常駐する前記秘密鍵を使用して受信された前記チャレンジに署名することによってそれぞれの前記チャレンジに応答し、署名された前記チャレンジを返すネゴシエーション手段と、

受信された前記チャレンジ署名が前記受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証し、前記第１装置と前記第２装置との間で鍵合意を確立し、前記検証のすべてに成功する場合にセキュア通信を確立する手段と

を含むシステム。

【請求項３５】

前記保護された記憶装置が読取書込記憶装置であり、前記記憶装置の読取が共用される秘密によってのみアクセス可能となっている、請求項３４に記載のシステム。

【請求項３６】

サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするシステムであって、前記サーバが組込み無線機モジュールを有し、

前記組込み無線機モジュールを使用して、前記サーバから前記第１装置に照会を送信し、前記第１装置から前記サーバに前記第１装置の固有装置識別子を返す通信手段と、

前記第１装置の公開鍵／秘密鍵対を作成する前記サーバ側のプロセッサと、

前記サーバで作成される前記第１装置の装置証明書であって、前記装置証明書が、前記第１装置に関連付けられた固有ハードウェア識別子および前記第１装置

に関連付けられた公開鍵を有する、装置証明書と

を含み、前記通信手段が前記第１装置に、前記秘密鍵、前記装置証明書、および前記装置証明書に署名した認証局の公開鍵を送信し、前記プロセッサが前記秘密鍵を前記第１装置の取外し不能な保護された記憶装置に記憶する

システム。

【請求項３７】

前記証明書のコピーが企業データベースに記憶される、請求項３６に記載のシステム。

【請求項３８】

前記証明書のコピーがＬＤＡＰディレクトリに記憶される、請求項３６に記載のシステム。

【請求項３９】

イニシャライズシステムであって、

組込み無線機モジュールを有する第１装置と、

組込み無線機モジュールを有するサーバと、

前記組込み無線機モジュールを使用して前記サーバから前記第１装置に照会を送信する通信手段とを含み、

前記第１装置が前記第１装置の公開鍵／秘密鍵対を作成し、前記秘密鍵を取外し不能な保護された記憶装置に記憶し、前記サーバに前記第１装置の固有装置識別子および前記公開鍵を返し、

前記サーバが、前記第１装置の装置証明書を作成し、前記装置証明書が、前記装置識別子および前記公開鍵を有し、前記サーバが、前記装置証明書および前記装置証明書に署名した認証局の公開鍵を前記第１装置に送信する

システム。

【請求項４０】

前記保護された記憶装置が前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、請求項３４、請求項３６、または請求項３９のいずれか一項に記載のシステム。

【請求項４１】

ユーザがセキュリティ関係を確立するシステムであって、

第１装置と、

第２装置と、

前記第１装置および前記第２装置のそれぞれに関する装置証明書であって、前記装置証明書のそれぞれが前記対応する装置の固有装置識別子を有する、装置証明書とを含み、

前記第１装置および前記第２装置の一方が前記装置の他方へのペアリング要求を開始し、前記第１装置から前記第２装置に前記第１装置の前記装置証明書を送信し、前記第２装置が前記第１装置の前記受信された装置証明書を暗号的に検証し、前記第１装置証明書に含まれる前記第１装置の前記装置識別子を出力し、前記ユーザが前記出力された装置識別子が前記第１装置の固有識別子と一致することを検証し、前記固有識別子が前記ユーザに既知であり、前記表示された装置識別子が検証される場合に、前記第１装置と前記第２装置との関連付けを受け入れる

システム。

【請求項４２】

前記送信および前記検証が前記第１装置と前記第２装置との間で認証されたセキュア・セッションを確立することによって達成される、請求項４１に記載のシステム。

【請求項４３】

前記第１装置および前記第２装置の関連付けのインジケータが長期記憶装置に配置される、請求項４１に記載のシステム。

【請求項４４】

前記インジケータが前記装置識別子である、請求項４３に記載のシステム。

【請求項４５】

前記インジケータが鍵材料である、請求項４３に記載のシステム。

【請求項４６】

前記ペアリング要求が前記装置の１つで入力選択を行うことによって開始される、請求項４１ないし４５のいずれか一項に記載のシステム。

【請求項４７】

前記ペアリング要求が前記装置の一方が前記装置の他方を自動的に検出することによって開始される、請求項４１ないし４５のいずれか一項に記載のシステム。

【請求項４８】

前記自動検出が前記装置の一方からの電磁信号の送信および前記装置の他方での前記電磁信号の受信によって達成される、請求項４７に記載のシステム。

【請求項４９】

前記関連付けの前記受け入れが前記第２装置で入力選択を行うことによって達成される、請求項４１に記載のシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、全般的には無線装置のセキュリティ管理に関し、具体的には、無線装置の間で情報をセキュアに伝送するセキュア短距離ネットワークの作成と、装置のペアリングのためのセキュア通信ネットワークの作成に関する。

【０００２】

【従来の技術】

コンピュータ・ネットワークでの無線装置の急増によって、装置の同期およびセキュア相互接続の大きな問題が生じた。ほとんどの無線装置は、現在、ディジタルであり、通信に電波を使用する。無線装置を使用する通常のユーザは、現在、ディジタル・メッセージを受信するポケット・ベル、ディジタル携帯電話、および電子メールを取り出し、送信する無線モデムを有するノートブック・コンピュータを有する。オフィスまたは他のネットワークに接続するために、ユーザがアクセスに慣れているリソースへの有線アクセスを可能にする広域ネットワークまたはローカル・エリア・ネットワークに接続するように設計された特殊なハードウェア（伝送機構を有するアダプタ・カードなど）が必要である。

【０００３】

モバイル通信とモバイル・コンピューティングの統合のために、標準規格が提案された。本明細書で「Bluetooth」と称するこの標準規格では、すべてのモバイル装置への小型で安価な無線機の組込みが提案される。この無線機は、標準規格に従って設計されるので、モバイル装置と無線機の組み合わせを、干渉を減らすように最適化することができる。この最適化が可能であるのは、現在無線アクセスに使用可能なさまざまな無線周波数バンドで別個の技術を使用する複数のオプション装置ではなく、単一の無線周波数バンドで実施される共通の無線プロトコルがあるからである。小型で低電力の無線機は、他の「Bluetooth」対応製品と通信するモジュールまたはチップで配布されることが意図されている。Bluetooth標準規格では、２つの選択された装置の間または複数の選択された装置の間での通信が定義されつつある。Bluetooth標準規格に関するさらなる情報は、ウ

ェブサイトhttp://www.bluetooth.comで入手可能である。

【０００４】

この標準規格では、現在、音声およびデータの両方の交換をサポートできる、使用可能な免許不要の２．４ＧＨｚ無線バンドの使用が定義されている。多数の一般的に合意された無線周波数で動作するが、この無線スペクトルの特定の部分は、低電力で免許不要の使用のために全世界で使用可能であると思われる。０－ｄＢｍ送信器を用いると、この低電力無線機は、約１０ｍの半径以内の装置のネットワークを確立するのに有効であり、距離が増加するにつれて急激に減衰する。２０－ｄＢｍ送信器を用いると、有効無線範囲が約１００ｍになる。この低電力無線機モジュールは、モバイル・コンピュータ、携帯電話機、3-in-1電話機、プリンタ、ファクシミリ機、モデム、ネットワーク・インターフェース（ＬＡＮ接続またはＷＡＮ接続など）、ディジタル・カメラ、ポケット・ベル、ヘッドフォンなどに組み込まれることが意図されている。非対称非同期データ伝送の場合の７２１Ｋｂｐｓまでの速度、または３つまでのアイソクロナス６４Ｋｂｐｓ音声チャネル、または合計１Ｍｂｐｓシンボル速度／ピコセル未満の音声チャネルとデータ・チャネルの組み合わせが、現在仕様によってサポートされており、技術の進歩に伴って通信速度が高まると期待される。Bluetoothでは、周波数ホッピングを使用するので、複数の調整されないピコセルが、お互いに近接する無線周波数内に共存することができる。

【０００５】

この仕様では、装置が相互作用する能力の大きな飛躍が記載されているが、装置のセキュア・チャネルの確立に関する大きい問題がまだある。この仕様書では、ハンド・ヘルド装置または無線装置が、「ピコネット」または「ピコセル」と称するものに接続することが許容される。ピコセルは、物理的に近接する（または小さい）ネットワークにすぎない。このピコネットによって、物理的に近接する装置（上で述べた無線範囲内）を相互接続するケーブルが置換される。Bluetooth無線機を有する「アクセス・ポイント」（または無線装置）によって、企業ＬＡＮまたはＷＡＮにピコセルを接続することができる。企業でのこれらの新しい装置の展開によって、複数の独自のセキュリティ問題および管理問題が明らか

になる。

【０００６】

上の仕様などの、この領域での従来技術では、装置のベースバンド（物理）層での認証および暗号化の方法が定義されているが、これらの方法は、今までに認識されていなかった制限を有し、これらの制限を下記で分析する。下記で説明する従来技術の方法のすべてが、認証および暗号化を実行するために適当な暗号手段と共に使用される秘密の暗号鍵を両方の装置にセキュアに提供するという目標を有する。これらの方法は、鍵を得る形に関して異なる。これらの方法は、鍵またはその先行ＰＩＮコードの再利用に関するポリシに関しても異なる。

【０００７】

従来技術が可能にする最初の通常の方法は、２つの装置が、ある指定されない外部の手段を介して、それらだけに知られる秘密の鍵を受け取ることである。この方法は、互いに永久的にペアリングされるように製造される２つの装置には適当である可能性がある。これらの装置は、この鍵を、パートナー装置の識別子に関連付けて記憶し、通信が望まれるたびにその鍵を再利用することができる。鍵を変更する方法が提供されない場合には、２つの装置は、互いに永久的にペアリングされ、製造の時点で異なる永久的な鍵を受け取った他の装置とは絶対にペアリングできない。鍵再利用のそのようなポリシの短所の１つは、２つの装置の間のセキュリティ関連付けが、永久的であることである。もう１つの短所は、第三者が、なんとかして鍵を知ることができた場合に、その後、自由に、もう１つの装置の偽名を使用するか、２つの装置を盗聴することが可能になることである。これらのシナリオのすべてで、初期のＲＦスペクトルでの無線周波数通信が、建物または壁などの視線をさえぎるものを貫通できるので、第三者は、観察されずに偽名を使用するか盗聴することもできる。

【０００８】

しばしば第１の方法より多少セキュアであると説明される第２の方法は、パーソナル・コンピュータとその無線マウス、またはセル電話機とその無線電話ヘッドセットなどの、長期的に互いに排他的にペアリングされる２つの装置に適する可能性がある。この方法では、両方の装置に、「ＰＩＮ」と称する同一の文字列

を与える必要がある。ＰＩＮは、製造業者が供給するか、ユーザが各装置で入力することができる。従来技術で、ＰＩＮをある既知の固定されたデータおよび一時的データと組み合わせて、後の認証および暗号化に使用される秘密の鍵を生成する方法が定義されている。それを行う方法の正確な詳細は、ここでは重要でない。長期間の「ペアリング」関係を作成することが望まれる装置の両方が、ペアリングされる装置に関連付けられた鍵を記憶する。鍵の生成に使用されたＰＩＮは、もはや不要になり、保存または破棄のいずれかを行うことができる。この記憶された鍵は、ペアリングされた装置がセキュアに通信することが望まれる時に、いつでも再利用される。装置の所有権が変更された場合には、前の鍵を削除し、新しいペアリング関係用のＰＩＮを入力し、新しい鍵を作成し、記憶することが可能である。この方法の短所の１つは、第三者が、言語による交換またはキーパッド入力の盗聴によるなど、なんとかしてＰＩＮを知った場合に、その第三者が、ペアリング・フローを盗聴することによって鍵を知ることができることである。鍵を知った後に、第三者は、別の装置の偽名を使用するか、暗号化された通信を盗聴することができる。

【０００９】

従来技術によって提供される第３の変形形態は、単一のトランザクションまたはデータ交換の持続時間の間だけお互いを信頼することを望む２つの装置に適当である可能性がある。この方法では、ユーザがトランザクションの直前に、両方の装置でＰＩＮを入力する。ＰＩＮは上と同様に鍵の生成に使用される。この鍵は、トランザクションの認証および暗号化に使用されるが、ＰＩＮと鍵の両方が、トランザクションの後に削除される。この２つの装置が、将来のある時に別のトランザクションを行うことを望まれる場合には、両方の装置をＰＩＮを用いてもう一度設定しなければならず、これはユーザにとって煩わしい処理である。

【００１０】

この第３の方法のよりセキュアでない変形形態では、装置にパートナー装置の識別子に関連付けられたＰＩＮが記憶されるが、使用後に鍵が削除される。したがって、この装置は同一のパートナーと通信する時に必ず同一のＰＩＮを再利用するが、各通信セッションの前に新しい鍵を生成する。この第３の方法は、鍵を

頻繁に変更して第三者がＰＩＮを知りペアリング・フロー中に盗聴することに成功する場合に第三者がセキュリティを侵害できる持続時間を制限することによって、第２の方法のセキュリティに対して改善される。

【００１１】

従来技術で既知の第４の方法は、ベースバンド認証および暗号化を要求するが、新しい通信セッションごとに０長ＰＩＮを使用して鍵を生成することである。この方法は、製品が、ユーザによる設定なしに、出荷用の箱から除去された時に即座に機能することを求め、最小限のレベルのセキュリティを提供することを望む製造業者によって選択される可能性がある。この手法の短所は、０長ＰＩＮが使用されていることを知っている第三者がペアリング・フローを盗聴して秘密の鍵を知ることができ、別の装置の偽名を使用したり、暗号化された通信を盗聴できるようになるという点で、第３の方法に類似する。

【００１２】

明らかに、非セキュア交換を介して鍵を得る方法は、偽名使用および盗聴の可能性を有する。現在の技術では、別の人に鍵またはＰＩＮ番号を言語で知らせるか、紙または電子メールを介して送達し、その結果、各装置でその装置のユーザが秘密を入力できるようにすることが提案される。この言語による交換、紙の交換、または電子メール交換が、第三者によって観察される場合に、秘密が危うくなる可能性がある。わずかな改良は、鍵またはＰＩＮの知識を単一の人に制限し、その人が両方の装置のキーパッドでそれを入力することである。これによって、鍵またはＰＩＮを盗み聞きするか見ることが排除されるが、キーパッド入力自体が、隠しカメラを使用することによるなど、第三者によって観察される可能性がある。非セキュアな形で交換されるデータを使用して通信セッションごとまたはトランザクションごとに秘密の鍵を生成する方法は、多少はよりセキュアであるが、悪意を持った第三者が鍵生成および交換の処理を盗聴する場合に、偽名使用および盗聴の対象になる。第三者が、なんとかして秘密を獲得した場合には、明らかに、秘密を再利用するというポリシが、秘密が絶対に再利用されない場合よりも高い潜在的な暴露を有する。

【００１３】

上で説明した従来技術のセキュリティ方法は、企業環境のモバイル・コンピュータにとって、不適切であり、煩わしく、役に立たない。本発明によって対処される、そのようなシナリオの例を、図５に示す。

【００１４】

図５には、通常の企業ＬＡＮ３０３に接続されたサーバ３０１が存在する。第２のサーバ３１１が、ＷＡＮを介して第１のサーバ３０１に接続され、通常の形でＬＡＮ３２１にも接続される。無線ノートブック・コンピュータ３１５などの無線装置を、サーバ３１１の無線アクセス・ポイントに接続することができる。無線装置は、エア・ウェーブを介してプリンタ３１３に直接に情報を送信することができる（情報をサーバ３１１に送信し、そのサーバに通常の有線接続を使用して情報をプリンタ３１３に送信させるのではなく）。

【００１５】

図５に示されたもう１つのシナリオには、無線ノートブック・コンピュータ３０９、電話機３０７、およびポケット・ベル３０５が含まれる。このシナリオでは、３つの装置のすべてが、通信することができ、電話機３０７またはポケット・ベル３０５が、無線ノートブック・コンピュータ３０９のディスクに関するログ記録のためにノートブック・コンピュータ３１９にメッセージを送信することができる。ビジネスの世界でのこれの現実的な例が、誰かが会議中であり、ある緊急の電子メールの到着を待っている場合である。システムは、新しい電子メールが無線ノートブック・コンピュータ３０９に（セル・モデムを介するか、ピコネットを介してノートブック・コンピュータに接続されたＬＡＮを介するなどして）到着した時に、電子メールの件名または送信者が無線ノートブック・コンピュータ３０９からポケット・ベル３０５にピコネットを介して送信され、ポケット・ベルが振動しメッセージを表示するようにセットアップすることができる。その代わりに、コンピュータが無線電話にダイヤルし、テキスト－音声変換機能を使用して、緊急の電子メールから読み上げることができる。もう１つの有用なシナリオは、ファクシミリ機３１７がノートブック・コンピュータ３１９への無線接続を有し、ノートブック機のユーザが、ファクシミリ機に接続された基礎となる電話網を使用して、モバイル・コンピュータにケーブルを挿抜する必要なし

に他者に情報を送信できるか、プリンタへの接続を有するサーバにアクセスできるというものであろう。この接続はノートブック・コンピュータ３１９とファクシミリ機３１７の間で無線によって直接に行われる。もう１つの有用なシナリオは、家庭内のケーブル・モデムまたはＡＤＳＬアダプタが無線トランシーバを備え、家庭内のすべてのタイプの装置、たとえばパーソナル・コンピュータ、電話ヘッドセット、テレビジョン受像機、ビデオ・レコーダ、オーディオ・スピーカ、およびオーディオ・レコーダなどが、無線接続によって有線ネットワークにアクセスできるというものである。これによって、ケーブルまたは構内配線の不便および出費なしに装置を簡単に追加または移動することができるという点で、ユーザに大きな便利さが提供される。また、製造業者またはサービス・プロバイダの観点からも、単一の物理アクセス装置での複数のサービスの統合が考慮されているので、これが望ましい。

【００１６】

従来技術が対処できない問題は、企業のシナリオを検討する時に極端に明白になる。本明細書で使用する「企業」は、通常は数千人ないし数十万人の従業員を有する非常に大きい会社または組織によって展開されるものなどの、非常に大規模のコンピュータ設備またはコンピュータ・ネットワークを指す。まさにそのサイズに起因して、または企業が複数の地理的位置でアクティブなので、企業は、しばしば、多数のより小さいサイトまたは数千人の従業員を収容する大きな敷地を有する。そのようなサイトおよび敷地は、一般に、ネットワーキング機能によって相互接続され、あるサイトから別のサイトに移動する従業員が、会社のどの位置でも自分の仕事に必要なアプリケーション・プログラム、リソース、データベース、および他のコンピュータ機能にアクセスできるようになっている。企業のシナリオでは、数千人ないし数十万人のユーザが無線装置を持って数ヵ所ないし数千ヵ所の間を移動し、各ユーザが所与の日全体を通じて計画されないアドホックな形で複数の装置に無線によって接続することを望む。本明細書で使用する「移動」は、ユーザが、自分自身および無線モジュールを含む自分のモバイル装置を、ある位置から別の位置へ物理的に移動することを指す。

【００１７】

パーソナル・コンピュータの複数機能特性（すなわち、ＰＣは、通常は、多数の異なるユーザの代わりに多数の異なる応用分野および装置に関するデータを交換する多数の異なるプログラムを実行する）のゆえに、パーソナル・コンピュータ・ユーザのセキュリティの必要は、完全に信頼されないものから完全に信頼されるものまでの全域を尽くし、これが事態をさらに複雑にする。前に説明した従来技術は、セキュリティ・ポリシを実施する複数の方法を提供するが、この企業コンテキストに関して満足なものはない。前に説明した技術のいずれかを、ネットワーク管理者が使用して、ネットワークへのアクセスを制限できるかどうかを考察する。

【００１８】

１．装置は、製造業者によって互いに永久的にペアリングすることができるが、柔軟性がなく、装置が複数の通信パートナーを有することができない。

【００１９】

２．装置は、たとえば共通のＰＩＮを両方の装置で入力し、それから記憶および再利用のために鍵を作成するか、通信セッションごとに新しい鍵を生成することによって、特定の他の装置との長期間のペアリング関係を有することができる。前にリストした短所のほかに、このポリシは、ＰＣが異なる通信パートナーに関する異なるセキュリティ・レベルを確立する要求を満足せず、また、同一のパートナーとの異なるトランザクションに関する異なるセキュリティ・レベルを確立する要求を満足しない。

【００２０】

３．管理者は同一のＰＩＮを用いてすべてのネットワーク・アクセス・ポイントを設定し、その後、そのＰＩＮをアクセスを許可されるすべての可能なモバイル・コンピュータ・ユーザに供給することができる。これによって、セット・アップすべきＰＩＮが１つだけになり（複数のアクセス・ポイントで行わなければならないが）、正しく設定されたＰＣが企業内のどこにでも移動でき、どのアクセス・ポイントを介してもアクセスを得ることができるようになるので、管理者の設定の労力が最小になるが、その秘密のＰＩＮが危険にさらされた場合に、悪意を持った第三者がすべてのアクセス・ポイントへのアクセスを得ることができ

る。許可された従業員が会社を辞めた場合に、その人のアクセスを取り消す簡単な方法はない。この方式は、非常に非セキュアなので許容不能である。

【００２１】

４．管理者は異なるＰＩＮを用いて各ネットワーク・アクセス・ポイントまたはアクセス・ポイントのグループを設定し、その後、許可されたユーザのある組にあるアクセス・ポイントのＰＩＮを供給することができる。許可されない人がＰＩＮを知った場合に、その人は、アクセス・ポイントの組へのアクセス権を得る。多数のモバイル・コンピュータでのＰＩＮのリストの管理が困難になる。ユーザのアクセス特権の取消は、ユーザがアクセス装置を持ち続ける場合に困難である。管理者は許可されないユーザを妨げるためにアクセス・ポイントのＰＩＮを変更することができるが、これによって、すべての許可されるユーザがその設定を同時に更新しなければならなくなる。管理者が新しいＰＩＮを有する新しいネットワーク・アクセス・ポイントの追加を望む場合に、許可されるユーザのすべてが通知されなければならず、かつ、自分のＰＣを更新しなければならない。アクセス・ポイントの異なるグループへのアクセス権を、たとえば旅行中にユーザに与えることは困難である。明らかにこの方式は使用不可能である。

【００２２】

５．管理者は各モバイルＰＣに固有のＰＩＮを割り当て、特定のアクセス・ポイントで許可されるＰＩＮのリストを設定することができる。管理はさらに困難になる。このリストにすべてのユーザが含まれる場合には、リストが管理不能に長くなる可能性があり、大量のＰＩＮを記憶するために追加メモリを設けなければならないので、アクセス・ポイント装置のコストが増える可能性もある。リストにユーザのサブセットが含まれる場合には、ユーザの移動する能力が制限される。ユーザの追加または除去が行われる場合に、管理者はすべての関連付けられたアクセス・ポイントで情報を更新しなければならない。この方法は、ある人がアクセス・ポイントのどれかで設定されたアクセス・リストの知識を得る場合に、その人が別の装置の偽名を使用するか別のユーザのＰＩＮを不正流用することによって複数のアクセス・ポイントへのアクセス権を得られることを除いて、比較的セキュアである。

【００２３】

前述から明白であるように、短距離無線の移動性は企業ネットワーク管理者に重大なセキュリティ課題を提示する。これは本発明によって対処される。

【００２４】

【発明が解決しようとする課題】

【課題を解決するための手段】

本発明は、無線機モジュールを含む無線装置を使用して、ディジタル証明書を使用してセキュアな形で接続できるようにする。本発明は、ユーザ識別子、パスワード、または暗号鍵の手入力を必要としない。本発明は、装置をイニシャライズするための追加の管理オーバーヘッドをもたらさずに、企業内のセキュア装置の効率的な管理も可能にする。本発明では、事前に構成された秘密の非柔軟性を除去し、秘密の手入力、記憶、または再利用に関連付けられたセキュリティ暴露を減らしながら、認証、暗号用の一時的暗号鍵のセキュアな生成および交換を行う方法、装置、およびプログラム製品と、企業内で別個のアクセス制御を実行し管理する手段とを説明する。

【００２５】

例のみを目的として、添付図面を参照して、本発明をこれから説明する。

【００２６】

【発明の実施の形態】

本発明の好ましい実施形態を提示して、本明細書を読んだ者が本発明を実施できるようにするのに十分な情報を提供する。どのような形でも、本発明を制限することは意図されていない。

【００２７】

Bluetooth仕様の設計者は、ベースバンド（または物理）層での認証および暗号化の実行を禁止しなかったが、そのような認証および暗号化をイニシャライズする現在の方法は、特に企業コンテキストでの、モバイル・コンピュータに許容不能な特性を有する。まだ、企業で効率的にセキュリティ（すなわち、認証、暗号化、アクセス制御、およびこれらの管理）を実施する方法に関する重大な混乱がある。誰が誰と対話でき、どの「共用される秘密」（ＰＩＮ番号、暗号鍵など

）が、特定の装置、ユーザ、アプリケーション、およびグループの間の接続を保護するのに使用されるかを定義する現在の方法論は、まだ存在しない。

【００２８】

企業では、セキュリティが、非常に大きな問題である。各アプリケーションならびに各装置が、異なるレベルのセキュリティを必要とする可能性があり、異なるレベルのセキュリティ・アクセスを可能にする能力が必要である。各トランザクションの前にＰＩＮを入力し、ＰＩＮまたは暗号鍵を絶対に記憶しないこと、またはすべてのトランザクションに同一の記憶されたＰＩＮまたは暗号鍵を使用することなどの両極端の企図されている解決策のどれもが許容不能である。記憶されたＰＩＮからオンザフライで一時的な新しい暗号鍵を生成するという中間のセキュリティ・オプションも、そのＰＩＮを知っている誰もがペアリング・フローを盗聴することによって潜在的に新しいリンク鍵を知ることができるので許容不能である。

【００２９】

本発明は、無線環境ならびに潜在的に他の環境でセキュアに通信するというこの問題および他の問題を解決する。本発明は、どのような形でも、この実施形態に制限されない。本発明は、装置が他の装置に頻繁にアクセスし、セキュアな形の識別または認証を必要とするすべてのモバイル環境、暗号化および他の目的に使用することができる暗号鍵のセキュアな生成および交換の方法、および、アクセス特権の追加、取消、または変更の能力を含む別個（すなわち、装置ごと、ユーザごと、グループごと、アプリケーションごと、またはトランザクションごと）のアクセス制御に同等に適用可能である。

【００３０】

本発明の好ましい実施形態には、ユーザおよび装置に関連付けられた証明書の組が含まれる。証明書には、図６に示されているように、少なくとも装置識別子４０１０、装置の公開鍵４０１５、およびオプションのデータ４０２０の区域が一般に含まれる。さらに、本発明の好ましい実施形態には中央管理されるアクセス制御データベースが含まれる。

【００３１】

従来技術では証明書が装置ではなく、ユーザまたは高水準アプリケーション・プログラムに関連した。したがって、ユーザは証明書をそれに対応する公開鍵と共にスマート・カードなどを介してワークステーションからワークステーションへ移すことができ、その証明書によってユーザが識別された（秘密鍵は、その使用を制御したユーザの代理である）。証明書の検証および妥当性検査は、通信装置の間のＴＣＰ／ＩＰフローを介して行われていた。本発明は、証明書を装置に、より具体的には、装置に含まれる無線機モジュールに密に結合し、その無線機モジュールの固有の識別子が証明書の固有の識別子として使用される。

【００３２】

本発明の好ましい実施形態では、提案される無線機モジュールを含む装置のそれぞれに証明書が割り当てられる。説明される例示的な証明書には、装置の固有の４８ビットＩＥＥＥ（ＭＡＣ）アドレス（任意の固有の識別子を同等に効果的に使用することができるが）、装置の公開鍵、有効性期間、および認証局からの署名が含まれる。本発明の好ましい実施形態では、装置識別子が証明書の「subject」フィールドに記憶される。各装置は、公開鍵／秘密鍵対も関連付けられ、前記公開鍵は上で述べた証明書に記憶されるものと同一の公開鍵である。装置はルート認証局の公開鍵またはチェーン許可チェーン内の認証局の公開鍵（本明細書ではＣＡの公開鍵と呼称する）も獲得しなければならず、その結果、装置が他の装置から受け取った証明書の認証性を検証できるようになる。認証局の署名によって、認証局が既知であり、信頼される場合に、装置識別子と装置証明書の公開鍵の間の関連を信頼できることが示される。認証局の公開鍵は、他の装置証明書の署名を検証するのに使用される。

【００３３】

公開鍵暗号の分野で周知の通り、公開鍵によって対応する秘密鍵によって暗号化されたデータを暗号化解除することができる。さらに、秘密鍵によって対応する公開鍵によって暗号化されたデータを暗号化解除することができる。また、ブロックに対するハッシュを計算し、署名者の秘密鍵を用いてハッシュを暗号化することによって、データのブロックに署名できることが周知である。署名は、署名者の公開鍵によって署名を暗号化解除し、その結果をデータ・ブロックの計算

されたハッシュと比較することによってテストすることができる。これらの値が一致する場合に、署名者が公開鍵に対応する秘密鍵を有することと、データ・ブロックが変更されていないことが示される。

【００３４】

本発明の好ましい実施形態では、秘密鍵の値が物理的に保護されるが装置に常駐するソフトウェアが秘密鍵の値を使用するディジタル署名動作を実行するようにハードウェアに要求できる形で、装置の秘密鍵がその装置に記憶される。これを達成する方法の１つが、書込専用記憶手段を使用し、装置に常駐するソフトウェアが鍵を読み取る方法がないが、装置が情報に対する動作を実行できるようにすることである。保護された値に対する動作の例が、秘密鍵の値を使用するディジタル署名動作である。この実施形態は好ましいが、情報を保護する他の手段を同様に適用可能である。たとえば、そのような物理的にセキュアな記憶の代替位置は、スマートカードまたはスマートカード・チップである。現在のスマートカード装置への記憶によって、正しいＰＩＮまたはパスワードが入力された場合に限ってデータに対する読取アクセスが可能になる。これは、従来技術よりはるかによい。というのは、従来技術ではアクセスされる装置のそれぞれについてパスワードまたはＰＩＮを入力する必要があるが、本発明のスマートカード実施形態では、装置イニシャライズ中に単一のパスワードまたはＰＩＮを１回入力することだけが必要であり、証明書がそれ以降のセキュア・トランザクションに使用されるからである。

【００３５】

まず、エンド・ユーザへの配布の前に企業などのセントラル・ポイントに引き渡される、組込み無線機モジュールと共に配布される装置をイニシャライズする方法を提供する。従来は、新しい計算装置または通信装置を企業で使い始める前に、ある人が、ネットワーク、データベース、サーバなどの特定の企業リソースに装置がアクセスできるようにするために装置の構成の管理手順を実行する。これは、ＰＩＮまたはパスワードを形成する数字の列などの秘密の情報を入力することによって達成される。これは、極端にエラーの傾向があり、退屈であり、時間がかかる作業である。本発明を使用すると、企業装置（無線機モジュールを含

む）の管理者が、企業装置の無線機と通信することができる無線機を有するサーバを使用する。サーバは企業装置が受け入れ可能な近接距離にある時にその装置への照会を実行する。企業装置は、その固有の装置識別子、好ましくは４８ビットＩＥＥＥ（ＭＡＣ）アドレスを返す。セキュア条件の下でサーバは企業装置の公開鍵／秘密鍵対および関連付けられた証明書を作成し、これらのデータ項目を、それのために作成された装置にセキュアに送信する。企業装置は、証明書（なんらかのタイプの記憶装置に）およびその秘密鍵（前に説明した保護された記憶装置に）を記憶する。証明書のコピーが企業データベースに置かれる。図１ないし３に、さらに詳細に情報のフローを示す。

【００３６】

高機能な装置の追加のセキュリティのために、上記のフローを変更し、その結果、装置が公開鍵／秘密鍵対を生成し、公開鍵だけを管理サーバに送信するようにする。この形で、秘密鍵が送信されずに装置上で作成され破棄される。さらに高いセキュリティのためには、装置上の特殊なメモリ（保護された記憶装置）を増補してこの鍵対生成を実行し、秘密鍵がその装置上のソフトウェアにも絶対に使用不能になるようにすることができる。

【００３７】

図１では、まず、イニシャライズを行う装置または管理サーバ１００１が、新しいモバイル装置１００３に照会を送信して（ステップ１０１０）、モバイル装置１００３の固有の識別子を要求する。モバイル装置１００３は、その固有の識別子１０１５を管理サーバ１００１に送信する（ステップ１０２０）。管理サーバ１００１側の管理者は、その後、モバイル装置によって送信された固有の識別子が、別の手段によってその装置に関して受け取られたもの（装置上で印刷された、装置に関する文書と共に送信されたなど）と同一であることを検証する。その後、管理サーバ１００１とモバイル装置１００３の間で接続が確立される。管理者は管理サーバ１００１とモバイル装置１００３の一方または両方でＰＩＮまたは暗号化鍵１０２５を入力し、従来技術のフローを使用して、装置イニシャライズのために一時的なセキュアなリンクを確立できるようにする（ステップ１０３０）。その結果、モバイル装置１００３と管理サーバ１００１の間のセキュア

接続がステップ１０３０で確立される。管理サーバ１００１は、モバイル装置１００３用の公開鍵／秘密鍵対を獲得または生成する（ステップ１０３５）。１０４５で、管理サーバ１００１が、作成された公開鍵１０４０を、前のフロー中に獲得されたモバイル装置１００３の固有の識別子１０１５と共に証明書要求メッセージ・バッファ１０５０に入れる。ステップ１０５５で管理サーバ１００１が認証局１００５へのセキュア接続を確立し、モバイル装置１００３のために準備された証明書要求１０５０を認証局に送信し（ステップ１０６０）、その結果、認証局１００５が認証局の秘密鍵を用いて証明書に署名し（ステップ１０６５）、署名された証明書を返す（ステップ１０７０）。管理サーバ１００１は、署名された証明書１０５０'を受信する時に、ステップ１０７５で、署名された証明書１０５０'を記憶する。図２を参照すると、管理サーバ１００１は、署名された証明書１０５０'および対応する秘密鍵（管理サーバが公開鍵／秘密鍵対を生成した場合）を、セキュア接続を介してモバイル装置１００３に送信し（ステップ１０８０）、認証局の証明書（ＣＡの公開鍵を含む）もモバイル装置１００３に送信し、セッションを終了する。署名された装置証明書およびそれに関連付けられた秘密鍵は、将来の使用のためにモバイル装置１００３内に記憶され（ステップ１０８５）、装置の秘密鍵がＣＡの公開鍵（他の装置の証明書の署名の検証に使用される）と共に保護された記憶装置に記憶され（ステップ１０９０）、装置証明書が適当な位置に記憶される。好ましい実施形態では、装置証明書のコピーが将来の参照のために企業アクセス制御データベースにも記憶される。ＰＩＮは、管理サーバ１００１とモバイル装置１００３の間の接続を保護するために共用された秘密なので、削除される（ステップ１０９５）。

【００３８】

上で指摘したように、企業装置がそれ自体の公開鍵／秘密鍵対を作成する適当な計算能力を有する場合には、図３に示されているように、フローのわずかな修正することが好ましい。管理サーバが公開鍵／秘密鍵対を生成するのではなく、モバイル装置１００３が、それ自体で公開鍵／秘密鍵対を生成し（ステップ１１１０）、その秘密鍵を保護された記憶装置に即座に記憶する（ステップ１１１５）。この場合、モバイル装置１００３の秘密鍵は絶対に誰にも送信されない。モ

バイル装置１００３は管理サーバとのセキュアまたは非セキュアの接続を確立し（ステップ１１２０）、その公開鍵だけを管理サーバ１００１に送信する（ステップ１１２５）。管理サーバ１００１は、やはり、公開鍵および装置識別子を証明書要求に入れ、そのデータを認証局１００５にセキュアに送信し、その結果、ＣＡがその秘密鍵を使用してディジタルに署名された証明書１０５０'を生成でき、署名された証明書を管理サーバ１００１に送り返せるようにし、署名された証明書を適当な記憶位置での記憶のためにセキュアまたは非セキュアの接続を介してモバイル装置１００３に送信するという、図１および図２で説明されたものと同一のステップを実行する。本発明のこの形態では、モバイル装置１００３がＣＡの公開鍵も取得し（ステップ１１３０）、前に説明した形で記憶しなければならない。

【００３９】

公開鍵、秘密鍵、および証明書を作成した後に、管理者は、ＩＢＭ社のOn-Demand Serverを用いて使用可能なものなどの標準的な配布技法を使用して、装置に特定のユーザまたはユーザのグループを関連付け、ユーザまたはユーザ・グループまたは装置にアクセス制御グループを関連付け、装置の装置特性をログ記録することができる。

【００４０】

上記の実施形態のもう１つの変形形態は、署名された証明書の拡張フィールドに追加データを含めることである。そのような拡張フィールドには、たとえば、ユーザ・グループ関連付け、アクセス制御グループなど、分離されたペアリング情況で自立的なアクセス・ポリシ決定を行えるようにするのに使用することができるものを含めることができる。

【００４１】

本発明を使用する無線接続が、まず、装置証明書を与えられた装置の対の間で確立される時の動作中には、認証および暗号化を当初はオフにすることができる。装置はＳＳＬ／ＴＬＳで、対称鍵合意に達するステップを含めてその間に流れる制御レコードに類似するプロトコルを使用して、お互いとの「ペアリング」関係を確立する。ＳＳＬ／ＴＬＳは鍵合意をもたらすことができる複数のオプショ

ンを提供し、そのいずれもが本発明による使用に適するが、好ましい実施形態は、Diffie-Hellman鍵合意である。ＳＳＬ／ＴＬＳ制御レコード・プロトコルは装置に互いに証明書を交換させ、どちらの装置でもＰＩＮまたは暗号鍵の入力および記憶なしに、また、暗号鍵またはＰＩＮを再利用する必要なしに、相互認証をもたらす。ＳＳＬ／ＴＬＳ制御レコードからとられるＳＳＬ鍵材料に対するＳＨＡ－１関数の実行とその後の必要に応じたｎバイトのサブセットの選択によって生成されるセッション鍵が、ペアリングされる装置のそれぞれによってそのローカル暗号化構成要素（好ましい実施形態のベースバンド・ファームウェアなど）に渡され、鍵合意に達したパートナーとの通信セッションの持続時間の間または鍵合意の持続時間の間の短い方、もしくは、アプリケーション、ユーザ、装置、および企業の要件に適する時間期間の間、リンク鍵として使用される。そのパートナーに関する生成された鍵を使用する暗号化が活動化される。セッションの進行中に鍵合意が満了した場合には、ペアリングされた装置は、前のセッション鍵を使用して暗号化されるか平文のいずれかで、同一のＳＳＬ／ＴＬＳ制御レコード・プロトコルを使用して、別の鍵合意を確立することができ、これによって前に説明したようにやはりそれぞれの暗号化構成要素に渡される新しいセッション鍵がもたらされる。ＳＳＬ／ＴＬＳは非常に完全にテストされセキュアであるとみなされるので好ましい実施形態について選択されるが、証明書交換および秘密鍵を使用してセッションを生成する方法であればどれでも使用することができる。もう１つの適する従来技術の方法が、ＩＥＴＦのIP Security Protocol（ＩＰＳｅｃ）作業グループによって、一連のＲＦＣ（Request for Comment）に記載されている。さらなる背景情報については、ＲＦＣ　２４１１「IP Security Document Roadmap」を参照されたい。

【００４２】

図４に本発明を使用する無線トランシーバをそれぞれが備える複数の装置の間でセキュア通信を確立する例のフローを示す。好ましい実施形態では、図１ないし３に関して前に説明したように、各装置にそれ自体の装置証明書、それ自体の秘密鍵、および認証局の周知の公開鍵が与えられた後に、図４のフローが発生する。しかし、本発明は、他の形でのデータ・アイテムの提供を排除しない。たと

えばノートブック・コンピュータである第１の装置２００３が、第２の装置２００１との通信を望む時に、第１の装置２００３が、第２の装置２００１に接続要求を送信する（ステップ２００５）。その後、非セキュア接続２０１０が第１の装置と第２の装置の間で確立される。その代わりに、２０１０を０長ＰＩＮなどのデフォルトＰＩＮを使用する認証されるか暗号化されるかその両方が行われる接続とすることができる。ＳＳＬ／ＴＬＳプロトコルの制御フローが本発明の好ましい実施形態で進行する際に、以下の機能が実行される（この制御フローの代わりに別のフローが使用される場合には、そのフローによって同一の機能が提供されなければならない）。ネゴシエーションが行われ、これによって、認証の必要およびタイプ、暗号化の必要、暗号アルゴリズムの詳細、および圧縮が行われる場合にその詳細について合意する（ステップ２０２０）。この使用に関して、認証は両方向（第１の装置と第２の装置の両方がお互いの識別を知る）であり、暗号化が要求される。アルゴリズムは、ベースバンド・ハードウェア／ファームウェアによって使用されるものであるか、ペアリングされる装置に存在する他の暗号化構成要素である。最後に圧縮がＮＵＬＬとして指定される。認証が進行する際に、特殊なメモリ（保護された記憶装置）が、第２の装置に対してローカル装置の識別を証明するために前記装置の秘密鍵（保護された値）を用いて署名するように要求され、特殊なメモリが、第２の装置の証明書を検証するためにＣＡの署名を検証するように要求され、その結果、前記証明書に含まれる公開鍵を信頼して、第２の装置の署名を検証できるようになる。どこかの点で、パートナーの認証に失敗する場合に、セッションが打ち切られる。暗号化を要求した結果として、セキュアな形でセッション鍵が合意され（ステップ２０３０）、この点で、ＳＳＬ／ＴＬＳプロトコルまたは同等物が、ベースバンド・トランスポート（または他の適するローカル暗号化構成要素）のイニシャライズに使用される合意されたセッション鍵２０３５によって打ち切られて、その後の暗号化された動作が可能にされる（ステップ２０４０）。

【００４３】

上で説明した認証のフローは、両方の装置の証明書の交換および妥当性検査をもたらす。これは、これらの証明書のオプションの拡張フィールドが、ポリシ決

定のために使用可能であることを意味する。たとえば、第２の装置２００１は、第１の装置２００３の検証された証明書の内容に基づいて、必要な装置識別子またはオプションの（個別の名前またはグループ名に関連付けられた）証明書フィールドを使用してローカルのまたは企業のアクセス制御データベースに問合せ照会して、第１の装置２００３による暗号化された接続を介してどのリソース／機能を働かせることができるかを決定することができる。このすべてが、装置の間の直接のネゴシエーションによってセキュアに達成され、前に説明した、図１ないし３の１回だけのイニシャライズ手順または、各装置に装置証明書、秘密鍵、および認証局の公開鍵を与える同等の手順以外の、ユーザまたは管理者の側でのユーザ識別子およびパスワード、ＰＩＮ、または暗号化鍵などの各潜在的な通信パートナーに関連付けられた秘密の入力または記憶を必要としない。

【００４４】

好ましい実施形態では、装置が、サーバ側のアクセス制御データベースに登録されるので、証明書によって、サービスおよびリソースへのアクセスの制御ならびに、特定のタイプの表示のためのデータ・ストリームのフォーマットまたは特定のデータ・レコードへのアクセスの使用可能化などの、装置のために使用可能にしなければならない設定の選択の方法が提供される。本発明で説明される認証の方法を使用するモバイル装置が、それに割り当てられたユーザによって紛失された場合に、その装置の証明書を取り消すことができる（クレジット・カード発行者が、盗まれたクレジット・カードを当日に取り消すのと同様に）。ディレクトリまたはデータベースなどの企業のセントラル・ロケーションでの証明書取消は、他の装置での認証プロトコルがそのディレクトリまたはデータベースとの相互作用を必要とする場合に限って有効である。認証が中央のディレクトリまたはデータベースへのアクセスを必要としない切断モードでの、取消およびアクセスの拒否の最も有効な方法は、装置証明書を満了させ、装置のユーザに、装置証明書を周期的に更新することを要求することである。有効性期間フィールドが、前に述べたように、この目的のために証明書に設けられる。図７および図８に、これを詳細に示す。

【００４５】

図７に、モバイル装置１００３が第１のリソース５００１へのアクセスを要求する、中央アクセス制御を示す。モバイル装置１００３および第１のリソース５００１は、相互認証を実行し、暗号化をネゴシエートする（ステップ５０１０）。モバイル装置１００３は、その後、１つまたは複数のリソースへのアクセスを要求する（ステップ５０２０）。第１のリソース５００１は、モバイル装置１００３に関する認証の要求５０３０を認証局１００５である中央ディレクトリまたはデータベースに送信する。アクセスは、中央データベースまたはディレクトリの情報に基づいて許可または拒否される（ステップ５０５０）。

【００４６】

図８に、２つの装置すなわちモバイル装置１００３および第１のリソース５００１が、相互に認証し、暗号化をネゴシエートし（ステップ５０１０）、モバイル装置１００３が、リソースへのアクセスを要求する（ステップ５０２０）切断モードのアクセス制御を示す。しかし、切断されたシナリオでは、受信側の第１のリソース５００１が、暗号化された証明書のオプションのデータを検査する（ステップ５１００）。このデータの検査時に、第１のリソース５００１は、証明書のフィールドおよびローカルに記憶された情報に基づいてアクセスを許可するかどうかに関する決定を行う（ステップ５１１０）。証明書のフィールドには、証明書の満了日などの情報を含めることができる。要求された情報へのアクセスは、前と同様であるが、このローカルに得られた情報に基づいて、許可または拒否される（ステップ５１５０）。

【００４７】

本発明を使用すると、第１の装置は、次の３つの文が真である場合に認証される：（１）その証明書チェーンが、信頼されるＣＡ署名者（図２で記憶されたＣＡ公開鍵によって表される）が見つかる点までさかのぼってめいめいに含まれる署名を検査することによって検証することができ、（２）第１の装置がその証明書に含まれる公開鍵に関連付けられた秘密鍵を所有することを実証することができ、（３）証明書に記憶された装置識別子が、装置の実際の装置識別子と一致する（視覚的にまたは標準的な通信フローからなどの他の手段によって確かめることができる）。好ましい実施形態では、第１の装置がＳＳＬ／ＴＬＳまたは同等

のプロトコルの制御レコード・フロー内のチャレンジの署名によって、一致する秘密鍵を所有することを証明する。詐称者が保護されない記憶装置から第１の装置の証明書を盗み、第１の装置のＭＡＣアドレスを知るために盗聴することができる。その後、詐称者は固有の識別子（ＭＡＣアドレス）をスプーフィングし、その証明書を再生することによって第１の装置の偽名使用を試みることができるが、詐称者は、保護された記憶装置内で秘密に保たれる第１の装置の秘密鍵を得る方法を有しておらず、したがって、チャレンジに署名することができない。

【００４８】

本発明が有用になる可能性がある他の例には、図９に示されているように、ヘッドセットなどの装置を携帯電話に関連付けるなど、ＰＩＮまたは暗号化鍵の入力を伴わない装置の間の長期間のセキュア・ペアリング関係の作成が含まれる。これは、次のように達成することができる。ユーザがそれらの間でセキュア関係を確立することを望む２つの装置（６００１および６００３）を有する。各装置は、前に説明したように、装置識別子または通し番号を含む装置証明書を与えられ、この装置識別子または通し番号は、外部から見えるかなんらかの外部手段を介しても知られる。装置証明書、一致する秘密鍵、および認証局の公開鍵を管理者が生成する代わりに、これらのデータ項目を、製造業者が事前にインストールすることができる（ステップ６０１０）。装置は、イニシャライズされない（ペアリングされない）状態すなわち、リンク鍵、ＰＩＮ、またはペアリング関係を定義されずに、製造業者によって出荷される。２つのペアリングされていない装置を無線近接にして、ユーザは、装置がペアリングされていない時に特別な機能を実行するボタンを押す（ステップ６０２０）。これによって、装置が、図４に関して説明したように、その証明書をもう一方の装置に送信する（ステップ６０３０）。２つの装置の少なくとも１つが、ペアリングされる装置の識別子を表示する（ステップ６０４０）ことができる表示装置を有する必要がある（聞き取り可能な手段または他の出力手段を使用する装置を排除するものではない）。ディスプレイを有する装置は、認証局の公開鍵を使用して証明書チェーン認証性を検査することによって、他方の証明書を検証する。証明書の装置識別子が、装置の外側に書かれるか他の外部手段を介して知られる装置識別子と一致する場合に、

その識別子は真正である（ステップ６０５０）。ユーザが、ボタンを押し（ステップ６０６０）（選択を行う他の手段を排除するものではない）、装置がペアリング関係を受け入れ、装置識別子（または、任意選択としてリンク鍵）が、永久的記憶装置または長期記憶装置（ローカル・アクセス制御データベースを表すフラッシュＲＡＭまたは類似する記憶装置）にセットされる。証明書が装置識別子と一致しない場合にはユーザがペアリングを拒否し、動作が打ち切られる（ステップ６０７０）。ここで、２つの装置がペアリングされ、将来のどの時でもセキュアに再認証（証明書または任意選択で共用される秘密としてリンク鍵を使用して）し、暗号化された通信を確立することができる。これによって、製造業者が、生産プロセス全体を通じて装置の製造を同期化する必要なしに、装置を一意にペアリングできるようになる。ペアリングされた装置の所有者が、その装置の所有権を別の人に譲渡することを選択した場合には、所有者はペアリング関係を削除することができ、将来の所有者は前に説明したものと同一のステップを実行することによって、その装置の新しいペアリング関係を確立することができる。

【００４９】

まとめとして、本発明の構成に関して以下の事項を開示する。

（１）第１装置と第２装置との間でセキュア通信をイニシャライズする方法であって、第１装置および第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、装置証明書がそれぞれの装置に関連付けられた固有ハードウェア識別子およびそれぞれの装置に関連付けられた公開鍵を有し、

第１装置と第２装置との間のセッションを確立するステップと、

第１装置と第２装置との間で両方向セッション暗号化および相互認証要件をネゴシエートするステップと、

第１装置および第２装置の装置証明書を交換するステップと、

認証局の公開鍵を使用して受信された証明書を暗号的に検証するステップと、

第１装置および第２装置のそれぞれによって作成されたチャレンジを交換するステップと、

受信側装置の秘密鍵を使用して受信されたチャレンジに署名することによってそれぞれのチャレンジに応答するステップであって、秘密鍵が各装置の保護され

た記憶装置それぞれに常駐する、ステップと、

署名されたチャレンジを返すステップと、

受信されたチャレンジ署名が受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証するステップと、

第１装置と第２装置との間で鍵合意を確立するステップと、

検証するステップのすべてに成功する場合にセキュア通信を確立するステップと

を含む方法。

（２）保護された記憶装置が読取書込記憶装置であり、記憶装置の読取が共用される秘密によってのみアクセス可能となっている、上記（１）に記載の方法。

（３）サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズする方法であって、サーバが組込み無線機モジュールを有し、

組込み無線機モジュールを使用して、サーバから第１装置に照会を送信するステップと、

第１装置からサーバに、第１装置の固有装置識別子を返すステップと、

サーバで、第１装置の公開鍵／秘密鍵対を作成するステップと、

サーバで、第１装置の装置証明書を作成するステップであって、装置証明書が第１装置に関連付けられた固有ハードウェア識別子および第１装置に関連付けられた公開鍵を有する、ステップと、

第１装置に、秘密鍵、装置証明書、および装置証明書に署名した認証局の公開鍵を送信するステップと、

秘密鍵を第１装置の取外し不能な保護された記憶装置に記憶するステップと

を含む方法。

（４）証明書のコピーが企業データベースに記憶される、上記（３）に記載の方法。

（５）証明書のコピーがＬＤＡＰディレクトリに記憶される、上記（３）に記載の方法。

（６）サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズする方法であって、サーバが組込み無線機モジュールを有し、

組込み無線機モジュールを使用して、サーバから第１装置に照会を送信するステップと、

第１装置で、第１装置の公開鍵／秘密鍵対を作成するステップと、

第１装置で、秘密鍵を取外し不能な保護された記憶装置に記憶するステップと、

第１装置からサーバに、第１装置の固有装置識別子および公開鍵を返すステップと、

サーバで第１装置の装置証明書を作成するステップであって、装置証明書が装置識別子および公開鍵を有する、ステップと

装置証明書および装置証明書に署名した認証局の公開鍵を第１装置に送信するステップと

を含む方法。

（７）保護された記憶装置が前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、上記（１）、上記（３）、または上記（６）に記載の方法。

（８）第１装置と第２装置との間でセキュリティ関係を確立する方法であって、第１装置および第２装置がそれぞれ関連付けられた装置証明書を有し、装置証明書のそれぞれが対応する装置の固有装置識別子を有し、

装置の一方の装置の他方へのペアリング要求を開始するステップと、

第１装置から第２装置に、第１装置の装置証明書を送信するステップと、

第２装置によって、第１装置の受信された装置証明書を暗号的に検証するステップと、

第２装置で、第１装置証明書に含まれる第１装置の装置識別子を出力するステップと、

ユーザによって、出力された装置識別子が第１装置の固有識別子と一致することを検証するステップであって、固有識別子がユーザに既知である、ステップと、

ユーザによって、表示された装置識別子が検証される場合に、第１装置と第２装置との関連付けを受け入れるステップと

を含む方法。

（９）送信するステップおよび検証するステップが、第１装置と第２装置との間で認証されたセキュア・セッションを確立することによって実現される、上記（８）に記載の方法。

（１０）第１装置および第２装置の関連付けのインジケータが長期記憶装置に配置される、上記（８）に記載の方法。

（１１）インジケータが装置識別子である、上記（１０）に記載の方法。

（１２）インジケータが鍵材料である、上記（１０）に記載の方法。

（１３）ペアリング要求が装置の１つで入力選択を行うことによって開始される、上記（８）ないし（１２）のいずれか一項に記載の方法。

（１４）ペアリング要求が装置の一方が装置の他方を自動的に検出することによって開始される、上記（８）ないし（１２）のいずれか一項に記載の方法。

（１５）自動検出が装置の一方からの電磁信号の送信および装置の他方での電磁信号の受信によって達成される、上記（１４）に記載の方法。

（１６）関連付けの受け入れが第２装置で入力選択を行うことによって達成される、上記（８）に記載の方法。

（１７）第１装置と第２装置との間でセキュア通信をイニシャライズするコンピュータ・プログラムであって、第１装置および第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、装置証明書がそれぞれの装置に関連付けられた固有ハードウェア識別子およびそれぞれの装置に関連付けられた公開鍵を有し、装置に、

第１装置と第２装置との間のセッションを確立する手順と、

第１装置と第２装置との間で両方向セッション暗号化および相互認証要件をネゴシエートする手順と、

第１装置および第２装置の装置証明書を交換する手順と、

認証局の公開鍵を使用して受信された証明書を暗号的に検証する手順と、

第１装置および第２装置のそれぞれによって作成されたチャレンジを交換する手順と、

受信側装置の秘密鍵を使用して受信されたチャレンジに署名することによって

それぞれのチャレンジに応答する手順であって、秘密鍵が各装置の保護された記憶装置それぞれに常駐する手順と、

署名されたチャレンジを返す手順と、

受信されたチャレンジ署名が受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証する手順と、

第１装置と第２装置との間で鍵合意を確立する手順と、

検証するステップのすべてに成功する場合にセキュア通信を確立する手順と

を実行させるコンピュータ・プログラム。

（１８）保護された記憶装置が前に書き込まれたデータを用いる計算を実行する能力を有する書込専用記憶装置である、上記（１７）に記載のコンピュータ・プログラム。

（１９）保護された記憶装置が読取書込記憶装置であり、記憶装置の読取が共用される秘密によってのみアクセス可能となっている、上記（１７）に記載のコンピュータ・プログラム。

（２０）サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするコンピュータ・プログラムであって、サーバが組込み無線機モジュールを有し、サーバおよび第１装置に

組込み無線機モジュールを使用して、サーバから第１装置に照会を送信する手順と、

第１装置からサーバに、第１装置の固有装置識別子を返す手順と、

サーバで、第１装置の公開鍵／秘密鍵対を作成する手順と、

サーバで、第１装置の装置証明書を作成する手順であって、装置証明書が、第１装置に関連付けられた固有ハードウェア識別子および第１装置に関連付けられた公開鍵を有する手順と、

第１装置に、秘密鍵、装置証明書、および装置証明書に署名した認証局の公開鍵を送信する手順と、

秘密鍵を第１装置の取外し不能な保護された記憶装置に記憶する手順と

を実行させるコンピュータ・プログラム。

（２１）証明書のコピーが企業データベースに記憶される、上記（２０）に記

載のコンピュータ・プログラム。

（２２）証明書のコピーがＬＤＡＰディレクトリに記憶される、上記（２０）に記載のコンピュータ・プログラム。

（２３）サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするコンピュータ・プログラムであって、サーバが組込み無線機モジュールを有し、サーバおよび第１装置に

組込み無線機モジュールを使用して、サーバから第１装置に照会を送信する手順と、

第１装置で、第１装置の公開鍵／秘密鍵対を作成する手順と、

第１装置で、秘密鍵を取外し不能な保護された記憶装置に記憶する手順と、

第１装置からサーバに、第１装置の固有装置識別子および公開鍵を返す手順と、

サーバで第１装置の装置証明書を作成する手順であって、装置証明書が装置識別子および公開鍵を有する手順と

装置証明書および装置証明書に署名した認証局の公開鍵を第１装置に送信する手順と

を実行させるコンピュータ・プログラム。

（２４）保護された記憶装置が、前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、上記（１７）、上記（２０）、または上記（２３）に記載のコンピュータ・プログラム。

（２５）第１装置と第２装置との間でセキュリティ関係を確立するコンピュータ・プログラムであって、第１装置および第２装置がそれぞれ関連付けられた装置証明書を有し、装置証明書のそれぞれが対応する装置の固有装置識別子を有し、装置に

装置の一方の装置の他方へのペアリング要求を開始する手順と、

第１装置から第２装置に、第１装置の装置証明書を送信する手順と、

第２装置によって、第１装置の受信された装置証明書を暗号的に検証する手順と、

第２装置で、第１装置証明書に含まれる第１装置の装置識別子を出力する手順

と、

ユーザによって、出力された装置識別子が第１装置の固有識別子と一致することを検証する手順であって、固有識別子がユーザに既知である手順と、

ユーザによって、表示された装置識別子が検証される場合に、第１装置と第２装置との関連付けを受け入れる手順と

を実行させるコンピュータ・プログラム。

（２６）送信する手順および検証する手順が、第１装置と第２装置との間で認証されたセキュア・セッションを確立することによって実現される、上記（２５）に記載のコンピュータ・プログラム。

（２７）第１装置および第２装置の関連付けのインジケータが長期記憶装置に配置される、上記（２５）に記載のコンピュータ・プログラム。

（２８）インジケータが装置識別子である、上記（２７）に記載のコンピュータ・プログラム。

（２９）インジケータが鍵材料である、上記（２７）に記載のコンピュータ・プログラム。

（３０）ペアリング要求が装置の１つで入力選択を行うことによって開始される、上記（２５）ないし（２９）のいずれか一項に記載のコンピュータ・プログラム。

（３１）ペアリング要求が装置の一方が装置の他方を自動的に検出することによって達成される、上記（２５）ないし（２９）のいずれか一項に記載のコンピュータ・プログラム。

（３２）自動検出が装置の一方からの電磁信号の送信および装置の他方での電磁信号の受信によって達成される、上記（３１）に記載のコンピュータ・プログラム。

（３３）関連付けの受け入れが第２装置で入力選択を行うことによって達成される、上記（２５）に記載のコンピュータ・プログラム。

（３４）第１装置と第２装置との間でセキュア通信をイニシャライズするシステムであって、第１装置および第２装置がそれぞれ認証局の公開鍵および装置証明書を有し、装置証明書がそれぞれの装置に関連付けられた固有ハードウェア識

別子およびそれぞれの装置に関連付けられた公開鍵を有し、

第１装置と第２装置との間のセッションを確立し、第１装置と第２装置との間で両方向セッション暗号化および相互認証要件をネゴシエートし、第１装置および第２装置の装置証明書を交換する通信手段と、

認証局の公開鍵を使用して受信された証明書を暗号的に検証する検証手段と、

第１装置および第２装置のそれぞれによって作成されたチャレンジを交換し、受信側装置の秘密鍵であって、各装置の保護された記憶装置それぞれに常駐する秘密鍵を使用して受信されたチャレンジに署名することによってそれぞれのチャレンジに応答し、署名されたチャレンジを返すネゴシエーション手段と、

受信されたチャレンジ署名が受信側装置によって前に送信されたチャレンジのチャレンジ署名であることを暗号的に検証し、第１装置と第２装置との間で鍵合意を確立し、検証のすべてに成功する場合にセキュア通信を確立する手段と

を含むシステム。

（３５）保護された記憶装置が読取書込記憶装置であり、記憶装置の読取が共用される秘密によってのみアクセス可能となっている、上記（３４）に記載のシステム。

（３６）サーバを使用して組込み無線機モジュールと共に配布される第１装置をイニシャライズするシステムであって、サーバが組込み無線機モジュールを有し、

組込み無線機モジュールを使用して、サーバから第１装置に照会を送信し、第１装置からサーバに第１装置の固有装置識別子を返す通信手段と、

第１装置の公開鍵／秘密鍵対を作成するサーバ側のプロセッサと、

サーバで作成される第１装置の装置証明書であって、装置証明書が、第１装置に関連付けられた固有ハードウェア識別子および第１装置に関連付けられた公開鍵を有する、装置証明書と

を含み、通信手段が第１装置に、秘密鍵、装置証明書、および装置証明書に署名した認証局の公開鍵を送信し、プロセッサが秘密鍵を第１装置の取外し不能な保護された記憶装置に記憶する

システム。

（３７）証明書のコピーが企業データベースに記憶される、上記（３６）に記載のシステム。

（３８）証明書のコピーがＬＤＡＰディレクトリに記憶される、上記（３６）に記載のシステム。

（３９）イニシャライズシステムであって、

組込み無線機モジュールを有する第１装置と、

組込み無線機モジュールを有するサーバと、

組込み無線機モジュールを使用してサーバから第１装置に照会を送信する通信手段とを含み、

第１装置が第１装置の公開鍵／秘密鍵対を作成し、秘密鍵を取外し不能な保護された記憶装置に記憶し、サーバに第１装置の固有装置識別子および公開鍵を返し、

サーバが、第１装置の装置証明書を作成し、装置証明書が、装置識別子および公開鍵を有し、サーバが、装置証明書および装置証明書に署名した認証局の公開鍵を第１装置に送信する

システム。

（４０）保護された記憶装置が前に書き込まれたデータを用いる計算を実行することができる書込専用記憶装置である、上記（３４）、上記（３６）、または上記（３９）のいずれか一項に記載のシステム。

（４１）ユーザがセキュリティ関係を確立するシステムであって、

第１装置と、

第２装置と、

第１装置および第２装置のそれぞれに関する装置証明書であって、装置証明書のそれぞれが対応する装置の固有装置識別子を有する、装置証明書とを含み、

第１装置および第２装置の一方が装置の他方へのペアリング要求を開始し、第１装置から第２装置に第１装置の装置証明書を送信し、第２装置が第１装置の受信された装置証明書を暗号的に検証し、第１装置証明書に含まれる第１装置の装置識別子を出力し、ユーザが出力された装置識別子が第１装置の固有識別子と一致することを検証し、固有識別子がユーザに既知であり、表示された装置識別子

が検証される場合に、第１装置と第２装置との関連付けを受け入れる

システム。

（４２）送信および検証が第１装置と第２装置との間で認証されたセキュア・セッションを確立することによって達成される、上記（４１）に記載のシステム。

（４３）第１装置および第２装置の関連付けのインジケータが長期記憶装置に配置される、上記（４１）に記載のシステム。

（４４）インジケータが装置識別子である、上記（４３）に記載のシステム。

（４５）インジケータが鍵材料である、上記（４３）に記載のシステム。

（４６）ペアリング要求が装置の１つで入力選択を行うことによって開始される、上記（４１）ないし（４５）のいずれか一項に記載のシステム。

（４７）ペアリング要求が装置の一方が装置の他方を自動的に検出することによって開始される、上記（４１）ないし（４５）のいずれか一項に記載のシステム。

（４８）自動検出が装置の一方からの電磁信号の送信および装置の他方での電磁信号の受信によって達成される、上記（４７）に記載のシステム。

（４９）関連付けの受け入れが第２装置で入力選択を行うことによって達成される、上記（４１）に記載のシステム。

【００５０】

この装置証明書に基づくイニシャライズの方法は、コードレス電話機のヘッドセットと電話機ベース・ステーション、パーソナル・コンピュータと無線オーディオ・ヘッドセット、パーソナル・コンピュータと無線マウスなどの長期間の排他的ペアリングを有する消費者向け装置に特に適する。

【図面の簡単な説明】

【図１】

組み込まれた無線機モジュールを有するモバイル装置と管理サーバの間の通常のセットアップ・フローを示す図である。

【図２】

組み込まれた無線機モジュールを有するモバイル装置と管理サーバの間の通常

のセットアップ・フローを示す図である。

【図３】

それ自体の公開鍵／秘密鍵対を生成するのに十分な計算能力を有するモバイル装置のイニシャライズフローを示す図である。

【図４】

本発明の好ましい実施形態での可能な認証のフローを示す図である。

【図５】

本発明を実施することができるサンプル・ネットワークのサブセットを示す図である。

【図６】

例示的な装置証明書レイアウトを示す図である。

【図７】

集中アクセス制御のフローを示す図である。

【図８】

切断モードを使用するアクセス制御のフローを示す図である。

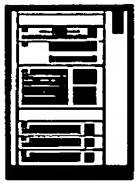
【図９】

装置証明書を使用する消費者向け装置のペアリングを示す図である。

【図１】


1003


1001


1005

照会する 1010

照会結果、識別子 1020

1015

PINを入力する 1025

セキュア接続を確立する 1030

1035 公開鍵／秘密鍵を生成する 1050

1045 証明書を作成する 1015 1040

1055 セキュア接続を確立する

1060 証明書を送信する

1050

A65 証明書に署名する

1070 署名された証明書を送信する

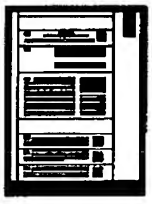
1050'

署名された証明書を保管する 1075

【図２】


1003


1001


1005

1080 証明書および鍵を送信し、切断する

署名された証明書および
公開鍵を保管する 1085

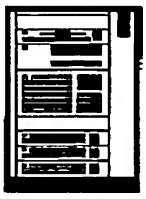
保護された値として
秘密鍵を保管する 1090

PINを削除する 1095 PINを削除する

【図３】


1003


1001


1005

照会する 1010

照会結果、識別子 1020

1015

公開鍵／秘密鍵対を
生成する 1110

秘密鍵をセキュアに
保管する 1115

接続を確立する 1120

公開鍵を送信する 1125

署名された証明書および
公開鍵を送信する

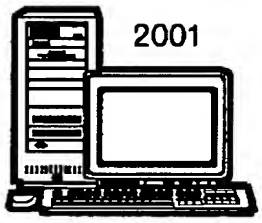
1050' 1130

図１および図２の
ステップと同一

【図４】


2003

認　証


2001

接続要求 2005

非セキュア接続 2010

制御レコード

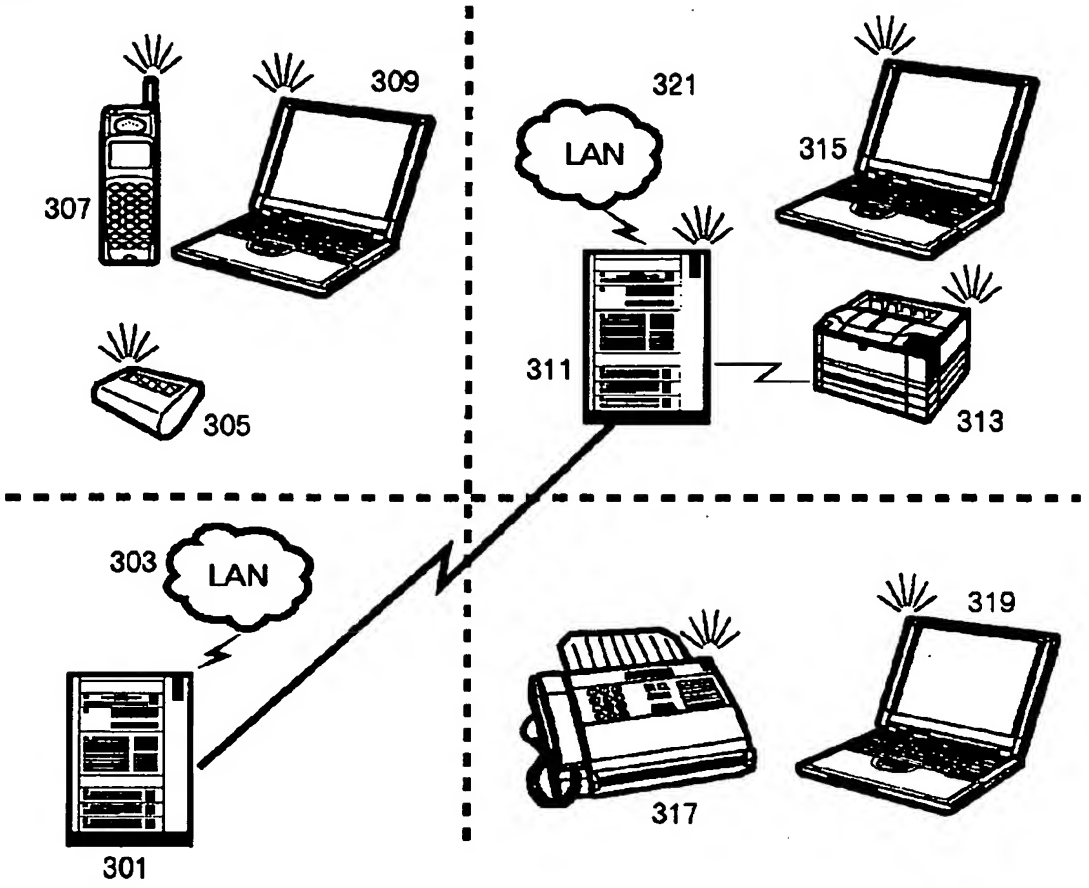
セッション鍵 2020

2030

セッション鍵を保管する 2035

暗号化を使用可能にする 2040

【図５】



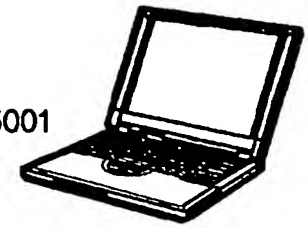
【図６】

装置識別子	4010
公　開　鍵	4015
オプションのデータ	4020

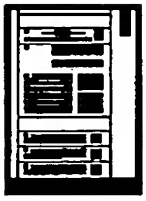
1050'

【図７】

1003



5001



1005

認証および暗号化　5010

アクセスを要求する　5020

認証を要求する　5030

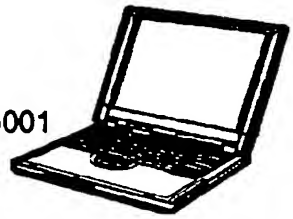
データベースに相談する　5040

認証されるか拒否される

認証されるか拒否される　5050

【図８】

1003



5001

認証および暗号化　5010

アクセスを要求する　5020

証明書のオプションの
データを検査する　5100

許可を決定する　5110

許可されるか拒否される　5150

【図９】

ヘッドセット 6001

6003

ペアリングされない
証明書が存在する 6010 ペアリングされない
証明書が存在する

ユーザがペアリングを
開始する 6020 ユーザがペアリングを
開始する

認証が進行する

6030

証明書からの装置IDを表示する 6040

ユーザが、表示された装置IDを
外部から供給される装置IDと比較する 6050

装置IDが一致する場合に、
ユーザがペアリングを受け入れる 6060

装置IDが一致しない場合に、
ユーザがペアリングを拒否する 6070

【国際調査報告】

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/GB 00/01940

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 197 30 301 C (DEUTSCHE TELEKOM MOBIL) 3 September 1998 (1998-09-03) abstract column 4, line 6 - line 25 column 4, line 42 - line 61 figures 1-3	1-3,8, 11,13, 14, 52-54, 64-66
A	US 5 621 798 A (AUCSMITH DAVID W) 15 April 1997 (1997-04-15) abstract column 2, line 26 - line 55 column 4, line 49 - line 62 column 5, line 56 - line 42 figures 2,5	1,8,11, 13,64

☐ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 September 2000	15/09/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int Ional Application No
PCT/GB 00/01940

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19730301 C	03-09-1998	AU 9252098 A	08-02-1999
		WO 9903285 A	21-01-1999
		EP 0995288 A	26-04-2000
US 5621798 A	15-04-1997	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(31)優先権主張番号　０９／３１６，６８６
(32)優先日　平成11年５月21日(1999. 5. 21)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＭＺ，ＳＤ，ＳＬ，ＳＺ，ＴＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＧ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＲ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＤＭ，ＤＺ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＡ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＭＺ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＴＺ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ
(72)発明者　ピーターズ、マーシャ、ランバート
アメリカ合衆国27614　ノースカロライナ州ローリー　ロチェガートン・レーン712
Ｆターム(参考)　5B085 AE29 BA06 BG02 BG07
5J104 AA16 EA02 EA04 EA26 JA21 MA01 NA03 NA05